



SUPPLY CHAIN MANAGEMENT and its RESPONSE
to TERRORISM
in
SRI LANKAN APPAREL SECTOR



University of Moratuwa, Sri Lanka
Electronic Theses & Dissertations
www.lib.mrt.ac.lk

By

Captain N Kuruparan

Supervised by

Dr P.Ramachandran

65'06'
62:65 (043)
TH

This dissertation was submitted to the Department of Management of Technology of the University of Moratuwa in partial fulfillment of the requirement for the degree of Master of Business Administration in Management of Technology

Department of Management of Technology

University of Moratuwa

November 2006

University of Moratuwa



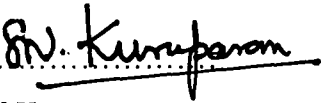
87882

87882

87882

DECLARATION

I hereby certify that this dissertation entitled "Supply Chain Management & it's Response to Terrorism In Sri Lankan Apparel Sector" is entirely my own work and it has never been submitted nor is it currently being submitted for any other degree. I also hereby give consent for my dissertation, if accepted, to be made available for photocopying and for interlibrary loans, and for the title and summary to be made available to outside organization.



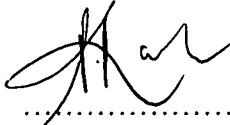
N Kuruparan

Captain – Sri Lanka Navy

Date: 31st Jan 2007



University of Moratuwa, Sri Lanka
Electronic Theses & Dissertations
www.lib.mrt.ac.lk



Dr. P Ramachandran

Date: 2nd Feb 2007

CONTENTS

	Page
DECLARATION	i
LIST OF CONTENTS	ii
LIST OF TABLES	vii
LIST OF ILLUSTRATION	viii
LIST OF ABBREVIATIONS	ix
ACKNOWLEDGEMENT	x
ABSTRACT	xi
1. INTRODUCTION	01
1.1 Background of the Research.	01
1.2 Problem Identification	04
1.3 Objectives of the Study	04
1.4 Scope and Limitation of the Study	05
1.5 Significance of the Study	06
1.6 Chapter Outline	06
2. LITERATURE REVIEW	08
3. METHODOLOGY	20
3.1 Context of Corporate Response Interviews	22
4. CORPORATE AND GOVERNMENT RESPONSES	23
4.1 Context of the Corporate Responses	23
4.1.1 Security principle	25
4.2 Insurance Industry Response - Insurance Coverage	26
4.2.1 Insurance industry risk assessment	26
4.3 Government Response	27

4.3.1	Infrastructure & interdependencies	27
4.3.2	Organizational – Ministry of Internal Security	28
4.3.3	Operational policy – Initiatives with industry	29
4.3.4	Issues with government response	30
4.4	Role of Technology	33
4.5	Mitigation Strategies	34
4.6	Learning from Past Events	35
4.7	Corporate Risk Assessment	35
4.7.1	Corporate threat perception	35
4.8	Supply Chains in a Vulnerable, Volatile World	36
4.8.1	Supply chains: Designed for a stable world	37
4.9	Old Threats and New	39
4.10	Managing Risks Strategically	40
4.11	Mapping Your Risk Profile	41
4.12	The Benefits of Risk Management	44
4.13	Corporate Risk Assessment Methods	48
4.13.1	Examples of risk assessment methodologies	49
4.13.2	Types of risks considered - Categorising risk	50
4.13.3	Focusing on failure modes	51
4.14	Modelling Risk of Terrorism	55
4.15	Quantifying the Impact: Making the Business Case	55
4.16	Cost or Collateral Benefit?	56
4.17	Who Pays and Who Decides ‘Standards of Care’?	58
4.18	Examples of Quantifying the Impact to Make the Business Case	60
4.19	Other Possible Risk Assessment Approaches	60
5.	APPAREL SECTOR RESPONSES – CASE OF SRI LANKA	62
5.1	Network – and not Firm Level – Security and Resilience.....	62
5.2	Resilience – Security	62
5.3	The Way Ahead: Creating the Resilient Supply Chain	63
5.3.1.	Supply chain (re) engineering	64

5.3.2.	Supply Chain Collaboration	67
5.3.3.	Agility	69
5.4.	Creating a Supply Chain Risk Management Culture	71
5.5	Supply Network Security	73
5.5.1	Physical security	73
5.5.2	Digital security	74
5.5.3	Summary security measures	75
5.6	Supply Chain Resilience - Today's Reality	76
5.6.1	Achieving resilience through flexibility and redundancy	76
5.6.2	Business continuity planning	78
5.6.3	Responses to create resilience by failure mode	80
5.6.4	Resilience to disruption in Supply	83
5.6.5	Resilience to disruption in transportation	86
5.6.6	Resilience to disruption in facilities	88
5.6.7	Resilience to disruption in communication	89
5.6.8	Resilience to disruption in human resources	90
5.7	Systems that Fail Smartly	91
5.8	Designing to 'Fail Smartly'	92
5.9	Supply Network vs. Integrated Supply Chain	92
5.10	Responding through Organization and Training	93
5.10.1	Creating a security ('socializing security') and resilience culture	93
5.10.2	Use of organizational design factors in Response	94
5.10.3	Educating and training the organization for security and resilience	95
5.11	A False Sense of Security and Confidence	96
5.12	Sole Source vs. Second Sources of Supply: Impact on Security and Resilience	96
5.13	Focus on physical security versus network security or business continuity	97
5.14	Apparel Sector Overview - Unplanned Exceptions Cripple Manufacturers	98
5.14.1	Supply net exceptions: A mess for manufacturers	98
5.14.2	Short term financial impact	99
5.14.3	High cost corrective measures	100

5.14.4	Undesirable side effects	100
5.15	Prevailing Supply Chain Habits and Tools don't Help	101
5.16	Manufacturers Must Embrace Uncertainty.	101
5.17	Firms will Learn to Turn Unplanned Events into Insight	102
5.18.	Supply Chain 'Security without tears'	108
5.18.1	Quality revolution to security of supply chain	108
5.18.2	Security perspective	109
5.18.3	Supply chain perspective	109
5.18.4	Win-Win principles	109
5.19	Mitigation Strategies	110
6.	COLLATERAL BENEFITS	117
6.1	Making the Case for Supply Chain Security Investments	117
6.1.1	Collateral benefits: A promising approach to ROI	118
6.1.2	The benefit: facilitating trade	119
6.1.3	Collateral benefits: A Promising Approach to ROI	119
6.2	Options to Create Additional Collateral Benefits	120
6.2.1	Collateral benefits from asset visibility and tracking	120
6.3	An Overview of Supply Chain Security Investment Options Offering Collateral Benefits	122
6.4	Collateral Benefits from Supplier Selection and Investment	122
6.5	Collateral Benefits from Transportation and Conveyance Security	123
6.6	Collateral Benefits from Building Organizational Infrastructure Awareness and Capabilities	124
6.7	Collateral Benefits from Collaboration among Supply Chain Parties	124
6.8	Collateral Benefits from Proactive Technology Investments	125
6.9	Collateral Benefits from Voluntary Security Compliance	126
6.9.1	Faster flow through customs	128
6.9.2	Potentially faster restart and flow through customs post disruption	129
6.9.3	Platform for collaboration	129
6.9.4	Supply chain efficiency	129
6.10	Broader Impact on the Apparel Firm	130

6.11	Achieving Collateral Benefits Connecting Security Investments and Collateral Benefits	131
6.11.1	Making the connection: Collateral benefits linkage maps	131
6.12	Challenges and Choices for Creating Collateral Benefits - Holistic Systems Approach?	132
6.13	Making Investment Choices	133
6.14	No More Tears	134
7	RECOMMENDATIONS AND CONCLUSIONS	135
7.1	Steps to Reduce Vulnerability	137
7.2	Resilience investment Justification	146
7.3	Disruption Response Canter.....	147
	LIST OF REFERENCES	149
	LIST OF APPENDICES	
	Appendix 1: The Nature of Apparel Markets	153
	Appendix 2: Supply Chain Mapping	161



University of Moratuwa, Sri Lanka.
Electronic Theses & Dissertations
www.lib.mrt.ac.lk

LIST OF TABLES

Table 1:	Supply Chain Security and Quality	24
Table 2:	Stages of Excellence	47
Table 3:	Self Assessment Score table	45
Table 4:	Self Assessment Table	48
Table 5:	Basic Supply Network Failure Modes	51
Table 6:	Supply Chain Security Measures	75
Table 7:	Supply Chain Resilience Responses by Failure Mode	81-82
Table 8:	Emerging Technologies Will Improve Firms' Supply Network Flexibility	107
Table 9:	Overview of a Range of Security Investments offering Collateral Benefits	121
Table 10:	Collateral Benefits from Building Organizational Infrastructure	
	Awareness and Capabilities	125
Table 11:	Security Investment Direct Benefits Collateral Benefits	127



University of Moratuwa, Sri Lanka.
Electronic Theses & Dissertations
www.lib.mrt.ac.lk

LIST OF ILLUSTRATION

Figure 1:	Research Methodology	20
Figure 2:	Martin Christopher & Helen Peck Model	65
Figure 3:	Supply Chain Knowledge	68
Figure 4:	Glitches are amplified throughout the supply network	99
Figure 5:	Technology Enabled Cycle	102
Figure 6:	Firms can Improve Learning by on Risk Root Causes	105
Figure 7:	Uses real options to increase its supply network	106
Figure 8:	Example of a Collateral Benefits Linkage Map	131
Figure 9:	Shorter life-cycle making timing crucial	153
Figure 10:	Inventory Hides Demand	155



University of Moratuwa, Sri Lanka.
Electronic Theses & Dissertations
www.lib.mrt.ac.lk

LIST OF ABBREVIATIONS

SCM	Supply Chain Management
DoD	Department of Defence
CTPAT	Custom-Trade Partnership Against Terrorism
USA	United States of America
EU	European Union
OEM	Original Equipment Manufacturers
SCOR	Supply Chain Operations Reference Model
SARS	Severe Acute Respiratory Syndrome
OSC	Op-Safe Commerce
CSI	Container Security Initiative
FAST	Free and Secure Trade
RFID	Radio Frequency Identification
VMI	Vendor Manage Inventory
CMI	Customer Managed Inventory
JIT	Just in Time
CPFR	Collaborative Planning, Forecasting and Replenishment
PEST	Political, Economic, Social and Technological
SCEM	Supply Chain Event Management
TQM	Total Quality Management
IT	Information Technology
IS	Information System
B2B	Business to Business
OS&D	Overages, Shortages, and Damages
SKU	Stores Keeping Unit

ACKNOWLEDGEMENT

I would like to take this opportunity to express my sincere thanks to Dr. P Ramachnadran Senior Lecturer Department of management of Technology (Project Supervisor) for his in valuable advice, understanding and encouragement given to me during this study. I would like to thank Dr. HSC Perera (Head of Department of Management of Technology), Dr Mrs V. Wickramasinghe, Mr Raj Prasana (Course Coordinator) for their timely guidance invaluable advice and support given through out the project.

I also with to thank the senior management of apparel sector companies for their valuable inputs and support during the project.

I wish to express my appreciation to the Sri Lanka Navy and in particular Commodore JC Hettigama, Director General, Electrical and Electronic Engineering Directorate for permitting me to follow the course.

I would also like to express my gratitude to the staff at Department of Management of Technology for valuable assistance rendered to me. Finally I would like to thank the Management of Technology faculty and all my colleagues who helped me to carry out this study and make it a success.

Finally, I lovingly and gratefully thank my beloved wife and children in helping and supporting my efforts to produce this research paper. Their sacrifice in fulfilling my ambition is appreciated.

ABSTRACT

The opening chapter dwells on how supply chain managers became aware of a new operating environment after the terrorist attacks on the World Trade Centre and the Pentagon on September 11, 2001. These events exposed the pre-existing and latent risk of disruption to supply networks from terrorist attacks. The risk was there all along but the attacks brought home the reality and the sheer vulnerability in everyone's minds. Sri Lanka is not different to USA. The country faces terrorist attacks to its infrastructure, business interests and key financial institutes such as the Central Bank of Sri Lanka. Furthermore, these events began to expose the total interdependence that exists between all firms in the supply network. The interdependence also includes reliance on those Sri Lankan Government agencies involved with inbound and outbound material flows and transportation infrastructure. Given these interdependencies, if one firm fails in the supply network, the entire network performance is at risk. Understandably, this constitutes a new operating environment where firms need to think in terms of their supply network and not just their individual performance.

The new operating environment calls for designing security and building resilience into the supply network. Security and resilience are unique characteristics that require distinct plans in order to develop and create these characteristics within the firm. Fortunately, there are several actions that firms can take which will contribute to both improved security and resilience. Improvement in security does not guarantee resilience. Neither does the addressing of resilience issues bring about security. The experience is that it is critical to design for both security and resilience.


New organizational capabilities are also called for in this environment. Specifically, firms will need to pioneer new relationships with Government agencies that now share responsibility for making the supply network secure and resilient. Additionally, firms will need to develop deeper relationships with suppliers and customers in their supply networks to jointly build a more secure and resilient network. Internally the largest organizational challenge may be in establishing at the individual level, a solid understanding of the interdependence of the systems, and the educational and training systems needed for robust network designs and

planned responses to disruptions. The Centre for Transportation and Logistics and the School of Management of Cranfield University prepared a practical guide and self assessment to understand the supply chain risks. This develops into the response to terrorist attacks and the change in the operating environment.

Redundancy, flexibility, vulnerability, visibility, velocity, acceleration, Collaborative planning and agility relationship are identified and extracted through an extensive literature survey described in chapter 2.

Chapter 3 describes the methodology of the research and the data and information collation procedures.

Past, present and future Corporate, Government and insurance industry responses to the terrorist disruption and natural disasters are identified. Also the risk identification methodologies, mapping risk, risk assessment and identifying benefits are discussed. The role of technology (Risk identification, analysis and mitigation) is also discussed in chapter 4.

 “Ultimately, you need to tie risk (of attack, disruption) to business performance.” Chapter 5 expands on these insights and builds a useful foundation for managers to use in designing their response in anticipation of future inevitable disruptions to the supply network by terrorism.

The final chapter lists the steps to reduce vulnerability, its justification and setting up of Distribution Response Centre.